



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **08251660 A**(43) Date of publication of application: **27.09.96**

(51) Int. Cl. **H04Q 7/38**
G06F 1/00
G06F 12/14

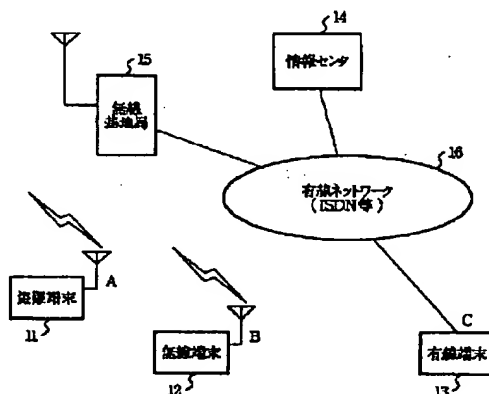
(21) Application number: **07052454**(71) Applicant: **NEC CORP**(22) Date of filing: **13.03.95**(72) Inventor: **ARIGA KENICHI**

(54) **SUBSYSTEM FOR PREVENTING ILICIT USE OF RADIO PORTABLE TERMINAL IN RADIO PORTBLE TERMINAL SYSTEM** COPYRIGHT: (C)1996,JPO

(57) Abstract:

PURPOSE: To disable the use of a stolen portable terminal by outputting a system lock request from a network to the terminal based upon information from an owner of the terminal and allowing the terminal to delete its all internal data.

CONSTITUTION: An owner of a stolen radio portable terminal 11 transmits information to which the terminal ID of the terminal 11 to an information center 14 through another radio portable terminal 12 or a wired terminal 13. The center 14 transmits an ID check request command to which the terminal ID of the terminal 11 is added through a radio base station 15. When a response is returned from the terminal 11, the center 14 transmits a system lock command to the terminal 11. Thereby the terminal 11 erases all the contents of an owner's personal data storage RAM backed up by a battery and then returns a system lock completion response to the center 14. The center 14 returns system lock completion information to the owner of the terminal 11.



JP-A 8-251660

Abstract

Purpose: To make a terminal unusable through network so as not to be used unfairly when the terminal is stolen in a radio portable terminal.

Constitution: An owner of a stole radio portable terminal makes burglary notice from the other terminal to an information center controlling the portable terminal. Receiving this notice, the information center sends system lock request to the objective terminal. Thus, the stole portable terminal deletes all internal data.

[0008]

Means for Solving Problem

The present invention prevents unauthorized access to network and reference of internal data by making the lost or stole radio portable terminal locking state (unusable state). Therefore, in a method for preventing unauthorized use of the radio portable terminal of the present invention, the above-mentioned object is achieved by making the portable terminal locking state with the use of means for noticing the effect from the owner to the portable terminal through radio network before the radio portable terminal obtained by third party is used unfairly.

[0009]

Operation

When the fact that burglary occurred is noticed to the information center, the information center finds the stole terminal and transmits request for deleting internal data to the stole terminal after confirmation of the party, thereby making the stole terminal system lock. Thus, unauthorized use of the stole portable terminal may be prevented.

[0010]

Example

A example of the present invention will now be described below with reference to the drawings.

[0011]

Fig. 1 is a constituent diagram of the system of the radio portable terminal system in which a subsystem for preventing unauthorized use of the radio portable terminal of the present invention is contained. Fig. 2 is a block diagram of the radio portable terminal of this system. Fig. 3 is a figure showing communication sequence between the radio portable terminal and the information center.

[0012]

First, constitution of hardware of the radio portable terminal will be described below with reference to the block diagram of Fig. 2.

[0013]

The radio portable terminal is comprised of a CPU 21 controlling the whole system, a ROM 24 in which control program and the like are stored, a RAM 22 for work that control program use, a RAM 23 for storing data in which personal data such as

directory, schedule and the like is stored, a display 25 for displaying information and operation, a input device 26 for inputting data and a radio module 27 for making control of radio.

[0014]

Data inputted by the input device 26 is stored in the RAM 23.

[0015]

Generally, since the RAM 23 is backed up by a battery, data therein is not deleted if power source is turned off. When data is transmitted with radio, data is sent from RAM 22, 23 and the ROM 24 to the radio module 27 through a system bus.

[0016]

Next, constitution of this system will be described below with reference to Fig. 1. The radio portable terminals A (11) and B (12) are registered in the information center 14. A wired terminal C (13) is a terminal capable of access to the information center 14. A radio base station 15 and the information center 14 are connected by wired network 16.

[0017]

Now, assuming that a certain person has the radio portable terminal A (11) and is robbed. The owner of the radio portable terminal A (11) accesses to the information center 14 by the terminal B (12) of the other person or the wired terminal C (13) in order to notice the fact that burglary occurred to the information center 14. The case where access is made by the wired terminal C (13) will be described below with the notice sequence diagram of Fig. 3.

[0018]

Connection request in which ID, a phone number and password are added is transmitted from the wired terminal c(13), and when the information center 14 receives it, the center returns connection completion response (301 in Fig. 3).

[0019]

After connection completion to the information center 14, notice of burglary in which terminal ID of the radio portable terminal A (11) is added is transmitted to the center 14 (302 in Fig. 3). The information center 14 which received notice of burglary returns command ascertainment response to the wired terminal C(13) and then transmits ID ascertainment request command in which ID of the stole terminal is added through the radio base station 15 in order to ascertain whether the stole terminal is in communication capable state (waiting state) (303 in Fig. 3). When the stole terminal A(11) is in communication capable state, ID notice response is returned.

[0020]

The information center 14 which ascertained ID notice response transmits system lock request command since the stole terminal A(11) is specified (304 in Fig. 3). The stole terminal A(11) which received this command deletes contents of the RAM 23 and then transmits system lock completion response to the information center 14.

[0021]

The information center 14 which ascertained system lock of the terminal notices the fact that the terminal became

locking state to the wired terminal C(13) by system completion notice (305 in Fig. 3). Here, since internal data of the stole terminal A(11) is deleted, security of the terminal is kept.
[0022]

Effect of the Invention

As described above, in the subsystem for preventing unauthorized use of the radio portable terminal of the present invention, since the terminal is made locking state by sending command from the owner to the terminal through radio network before the radio portable terminal obtained by third party is used unfairly, third party cannot access to radio network and refer internal data such as directory after lost or burglary of the portable terminal. Therefore, security of the terminal is kept.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-251660

(43) 公開日 平成8年(1996)9月27日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 Q 7/38			H 0 4 B 7/26	1 0 9 R
G 0 6 F 1/00	3 7 0		G 0 6 F 1/00	3 7 0 E
12/14	3 2 0		12/14	3 2 0 D

審査請求 有 請求項の数 2 O L (全 4 頁)

(21) 出願番号 特願平7-52454

(22) 出願日 平成7年(1995)3月13日

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 有賀 健一

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 弁理士 京本 直樹 (外2名)

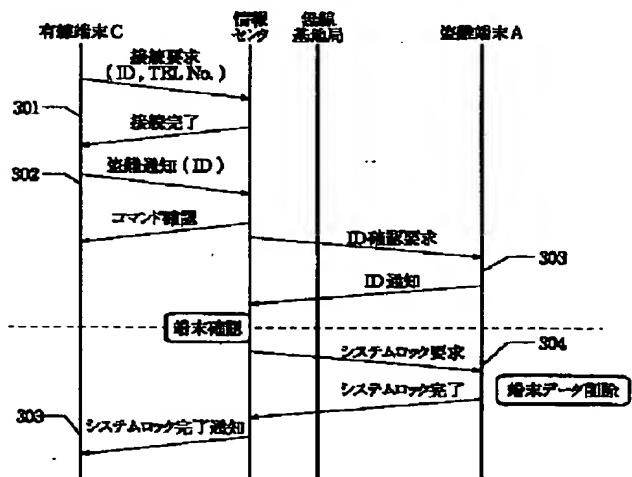
(54) 【発明の名称】 無線携帯端末システムにおける無線携帯端末不正使用防

止サブシステム

(57) 【要約】

【目的】 無線携帯端末において端末が盗難等にあった場合、不正使用されないようにネットワークを通じて端末を使用不能とする。

【構成】 盗難された無線携帯端末の所有者が他の端末より携帯端末を管理している情報センタに対して盗難通知を行い、この通知を受けて情報センタから対象となる端末に対してシステムロック要求を出す。これにより盗難された携帯端末は内部データをすべて削除する。



【特許請求の範囲】

【請求項 1】 情報センタに登録されサービスを受けている無線携帯端末システムにおける無線携帯端末不正使用防止サブシステムであり、

前記情報センタは携帯端末の盗難通知に応答して、前記携帯端末に対して内部データを消去する指示を送る手段を備え、

前記携帯端末は、前記情報センタからの消去指示に基づいて、その内部データを消去する手段と、

該内部データを消去完了した旨を情報センタに通知する手段とを備え、

前記情報センタは、前記携帯端末からの通知内容を盗難通知を発した端末に返す手段をさらに備えることを特徴とする無線携帯端末不正使用防止サブシステム。

【請求項 2】 前記情報センタは前記携帯端末の ID 確認要求を送信する手段をさらに含み、

前記携帯端末はこの ID 確認要求に応答して ID を情報センタに通知する手段をさらに含むことを特徴とする請求項 1 記載の無線携帯端末不正使用防止サブシステム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、無線携帯端末における不正使用に対するネットワークを介した防止方法に関する。

【0002】

【従来の技術】近年携帯端末が世の中に普及しつつあるが、携帯端末のセキュリティ確保についてはまだまだ発展途上段階にある。

【0003】従来の携帯端末の中には紛失したり盗難にあった場合のセキュリティを確保するために、パスワードを設定して起動時に入力させるようになっているものもある。

【0004】また特開平 5-94225 号公報は、パーソナルコンピュータに取り外し可能な IC カード等の不揮発性記憶装置を設け、カードが実装されていないとコンピュータそのものが起動しないようにすることによってセキュリティを保つ方法が記載している。

【0005】また特開平 5-145483 号公報は、起動時に所有者名を表示し、セキュリティコードと呼ばれるコードを入力しない限り所有者名の登録変更を禁止するという手段を有した無線端末を記載している。

【0006】

【発明が解決しようとする課題】無線携帯端末を紛失または盗難され、その端末を第三者が取得して不正に使用した場合、パスワード機能がなければ自由に無線ネットワークへのアクセスや住所録などの内部データの参照が可能である。またパスワード機能があっても、なんらかの手段によってパスワードを解読されれば、不正使用を防止することはできない。

【0007】本発明の目的は、盗難・紛失した無線携帯

端末が第三者によって不正使用されることを防止して、セキュリティの向上を図ることにある。

【0008】

【課題を解決するための手段】本発明は、紛失または盗難された無線携帯端末をロック状態（使用不可能な状態）とすることによって、ネットワークへの不正なアクセスや内部データの参照を防止する。このため本発明の無線携帯端末不正使用防止方法においては、第三者によって取得された無線携帯端末を、不正使用される前に所有者から無線ネットワークを通じて携帯端末にその旨を通知する手段により、携帯端末をロック状態にすることで上記目的を達成している。

【0009】

【作用】情報センタに盗難にあったことが通知されると、情報センタから盗難端末を探して、相手を確認した後に内部のデータを消去する要求を携帯端末に送信することによって、システムロックさせる。これによって盗難された携帯端末の不正使用を防止することができる。

【0010】

【実施例】以下、本発明の実施例について図面を参照して説明する。

【0011】図 1 は本発明の無線携帯端末不正使用防止サブシステムが収容される。説明する無線携帯端末システムのシステムの構成図であり、図 2 は本システムにおける無線携帯端末のブロック図であり、図 3 は無線携帯端末と情報センタとの通信のシーケンスを示す図である。

【0012】まず無線携帯端末のハードウェア構成を図 2 のブロック図を用いて説明する。

【0013】無線携帯端末はシステム全体を制御する CPU 21、制御プログラム等が蓄積されている ROM 24、制御プログラムが使用するワーク用 RAM 22、住所録やスケジュールなどの個人データを蓄積がされているデータ蓄積用 RAM 23、情報や操作を表示するための表示器 25、データを入力するための入力装置 26、無線の制御を行う無線モジュール 27 で構成されている。

【0014】入力装置 26 で入力されたデータはデータ蓄積用 RAM 23 に蓄積される。

【0015】一般的にデータ蓄積用 RAM 23 は電池でバックアップされているために、電源を落としても消去されることはない。無線でデータの送信を行う場合には、RAM 22、23、ROM 24 からシステムバスを通じて、無線モジュール 27 にデータを送ることにより行う。

【0016】次に本システムの構成を図 1 を用いて説明する。無線携帯端末 A (11)、B (12) は情報センタ 14 に登録されているものである。また有線端末 C (13) は情報センタ 14 にアクセス可能な端末である。無線基地局 15 と情報センタ 14 は有線のネットワ

3

ーク 16 で接続されている。

【0017】いまある人が無線携帯端末 A (11) を所有していて、盗難にあったと仮定する。無線携帯端末 A (11) の所有者は盗難のあったことを情報センタ 14 に通知するために、他の人の無線携帯端末 B (12) または有線の端末 C (13) を通じて情報センタ 14 にアクセスする。有線端末 C (13) でアクセスを行う場合を図 3 の通知シーケンス図を用いて説明する。

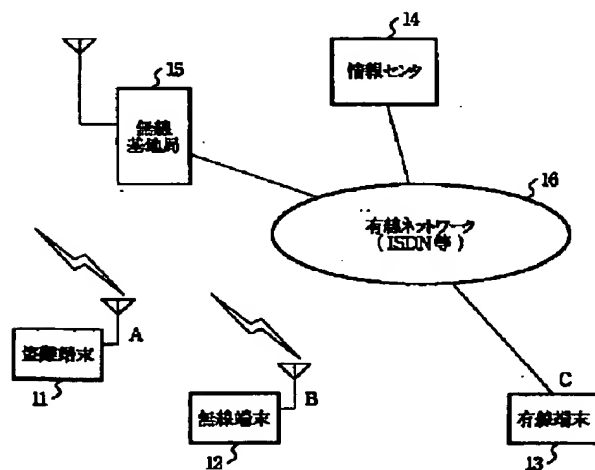
【0018】有線端末 C (13) から ID、電話番号、パスワードを付加した接続要求を送信し、情報センタ 14 が受け付けると接続完了レスポンスを返す (図中 301)。

【0019】情報センタ 14 に接続完了後、無線携帯端末 A (11) の端末 ID を付加した盗難通知を情報センタ 14 に送信する (図中 302)。盗難通知を受信した情報センタ 14 ではコマンド確認レスポンスを有線端末 C (13) に返した後、無線基地局 15 を通じて盗難端末が通信可能状態 (受け待ち状態) にあるかどうかを確認するために盗難端末の ID を付加した ID 確認要求コマンドを送信する (図中 303)。もし盗難端末 A (11) が通信可能状態であれば ID 通知レスポンスを返す。

【0020】ID 通知レスポンスを確認した情報センタ 14 では、盗難端末 A (11) が特定できたため、システムロック要求コマンドを送信する (図中 304)。このコマンドを受信した盗難端末 A (11) では、データ蓄積用 RAM 23 の内容を消去した後、システムロック完了レスポンスを情報センタ 14 に送信する。

【0021】端末のシステムロックを確認した情報センタ 14 では、その旨をシステムロック完了通知により有線端末 C (13) に端末がロック状態になったことを通

【図 1】



4

知する (図中 305)。ここで、盗難端末 A (11) の内部データは消去されたために端末のセキュリティが保たれることになる。

【0022】

【発明の効果】以上説明したように本発明の無線携帯端末不正使用防止サブシステムは、第三者によって取得された無線携帯端末を不正使用される前に所有者から無線ネットワークを通じてコマンドを送ることによって端末をロック状態にするために、携帯端末を紛失したり盗難にあった後に第三者が無線ネットワークへのアクセスや住所録などの内部データの参照することができなくなる。このため端末のセキュリティが保たれる。

【図面の簡単な説明】

【図 1】本発明の実施例のシステム構成図である。

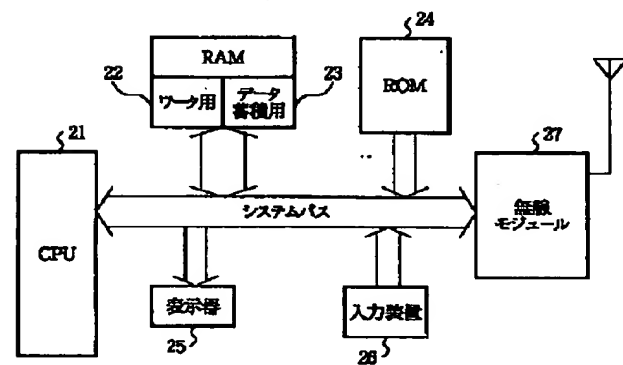
【図 2】本発明の実施例の端末のブロック図である。

【図 3】本発明の実施例の動作を示すシーケンス図である。

【符号の説明】

- | | |
|----|------------|
| 11 | 盗難端末 A |
| 12 | 無線端末 B |
| 13 | 有線端末 C |
| 14 | 情報センタ |
| 15 | 無線基地局 |
| 16 | 有線ネットワーク |
| 21 | CPU |
| 22 | ワーク用 RAM |
| 23 | データ蓄積用 RAM |
| 24 | ROM |
| 25 | 表示器 |
| 26 | 入力装置 |
| 27 | 無線モジュール |

【図 2】



【図3】

